What is claimed is:

1. A method for stopping Internet viruses from spreading via Email and Email attachments that damage computer systems. The said method comprising the steps of: inserting a routing in the program that receives Email and Email attachments that performs the function described in claim 2 and 3. inserting a second routine in the program that opens Email and Email attachments that performs the function described in claim 2 and 3, and inserting a third routine in the program that forwards Email and Email attachments that performs the function described in claim 2 and 3.

2. This method for stopping Internet viruses from spreading by Email is to move the first 64 bits of the data portion (note: this does not include the TCP/IP header) of the first packet of an Email to a created header for that Email. Then place a binary zero into the first 64 bits of the data portion of the first packet of the Email. By doing this, if someone sent a virus program in the Email, the first program instruction would be made a halt instruction and the program (virus) would not run. The flow chart for this procedure is in Figure 1.

Because the data has been changed after arriving into the computer the second routine gives the user an opportunity to replace the original data into the first 64 bits of the Email. This routine is detailed in figure 2.

To preserve data integrity, a third routine is provided to insure the original data is placed in the first 64 bits of the Email if one wants to forward the Email. This routine is described in figure 3.

3. This method for stopping Internet viruses from spreading by Email attachments is to

move the first 64 bits of the data portion (note: this does not include the TCP/IP header) of the first packet of the Email attachment to a created header for that attachment. Then place a binary zero into the first 64 bits of the data portion of the first packet of the Email attachment. By doing this, if someone sent a virus program in the Email attachment the first program instruction would be made a halt instruction and the program (virus) would not run. The flow chart for this procedure is in Figure 1.

Because the data has been changed after arriving into the computer the second routine gives the user an opportunity to replace the original data into the first 64 bits of the Email attachment. This routine is detailed in figure 2.

To preserve data integrity, a third routine is provided to insure the original data is placed in the first 64 bits of the Email attachment if one wants to forward the Email attachment. This is described in figure 3.